

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

9999 Fite Avenue, Hamersville, Ohio 45342

Case No.

1:18MJ-596

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

[SEE ATTACHMENT A]

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

[SEE ATTACHMENT B]

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

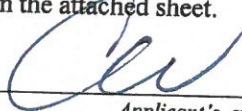
18 U.S.C. § 2252/2252A

Possession, Receipt & Distribution of Child Pornography

The application is based on these facts:

[SEE ATTACHED AFFIDAVIT]

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

CHRISTOPHER WALLACE, SPECIAL AGENT

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/1/18

City and state: CINCINNATI, OHIO



Judge's signature

HONORABLE KAREN L. LITKOVITZ

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH)
OF THE RESIDENCE LOCATED AT:)

9999 Fite Avenue)
Hamersville, Ohio, 45342)

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Christopher Wallace, Special Agent (S/A) with Homeland Security Investigations (HSI),
being duly sworn, depose and state as follows, to wit:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations (HSI), assigned to the Resident Agent in Charge field office in Cincinnati, Ohio. I have been so employed since May 2005. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants involving child exploitation and/or child pornography offenses.

2. This Affidavit is made in support of an application for a search warrant to search the residence of Wayne CUSIMANO and the entire premises located at 9999 Fite Avenue, Hamersville, Ohio 45342 (the SUBJECT PREMISES), more specifically described in Attachment

A, which is incorporated herein by reference. The purpose of this application is to seize evidence described in Attachment B of violations of Title 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography and access child pornography with intent to view it, and violations of Title 18 U.S.C. §§ 2252(a)(2)(B) and 2252A(a)(2), which make it a crime to receive and distribute child pornography.

3. As a federal agent, your Affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. The statements in this affidavit are based in part on information provided by law enforcement officers in Buffalo, New York and Boone County, North Carolina and on your affiant's investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact known to me concerning this investigation. Your affiant has set forth only the facts believed to be necessary to establish probable cause that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a) and 2252A, as further described in Attachment B are located at the SUBJECT PREMISES, as further described in Attachment A.

DEFINITIONS

5. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B (collectively referred to as "warrant"):

a. "Chat" refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation.

This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

- b. "Child Pornography" is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).
- c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. See Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis* (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. See *United States v. Cross*, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); *United States v. Riccardi*, 258 F.Supp.2d 1212 (D. Kan., 2003) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).
- d. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

- e. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- f. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).
- g. “Cloud-based storage service” refers to a publicly accessible, online, storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.
- h. “Computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).
- i. “Computer hardware” consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed

disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

- j. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic or other digital form. It commonly includes programs to run operating systems, applications and utilities.
- k. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.
- l. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- m. "File Transfer Protocol" ("FTP") is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
- n. "Internet Service Providers" (ISPs) are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means to access the Internet, including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- o. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers and other information, which may be stored both in computer data format and in written or printed

record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

p. "Internet Protocol address" (IP address) refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

q. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

r. The terms "records," "documents" and "materials" include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including writings, drawings, painting), photographic form (including microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including phonograph records, printing, typing) or electrical, electronic or magnetic form (including tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- s. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- t. “Digital device” includes any electronic system or device capable of storing and/or processing data in digital form, including the following: central processing units; laptop or notebook computers; PDAs; wireless communication devices such as telephone paging devices, beepers and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communications devices such as modems, cables and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips; and security devices.
- u. “Image” or “copy” refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. “Imaging” or “copying” maintains contents, but attributes may change during the reproduction.
- v. “Hash value” refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data.
- w. “Steganography” refers to the art and science of communicating in a way that hides the existence of the communication. It is used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file or other file format.

- x. "Compressed file" refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.
- y. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of `www.usdoj.gov` previously referred to the Internet Protocol address of `149.101.82.164`. Domain names are typically strings of alphanumeric characters with each level delimited by a period. Each level, read backwards from right to left further identifies parts of an organization. Examples of first level or top level domains are typically `.com` for commercial organizations, `.gov` for the governmental organizations, `.org` for organizations, and `.edu` for educational organizations. Second level names will further identify the organization. For example, `usdoj.gov` further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, `www.usdoj.gov` identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.
- z. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

- aa. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- ab. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper Text Mark up Language (HTML) and is transmitted from web servers to various web clients via Hyper Text Transport Protocol (HTTP).
- ac. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

BACKGROUND ON COMPUTERS, E-MAIL, THE INTERNET AND ONLINE CHILD EXPLOITATION

- 6. Based upon my knowledge, training and experience in online child exploitation and child pornography investigations, as well as the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following:
 - a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of online child exploitation. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, or directly from digital cameras. When a digital photo is taken, it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. Modems allow computers to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. CDs and DVDs are unique in that special software must be used to save or "burn" files onto them. Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet, the World Wide Web and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.

f. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any

computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. And even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most cases.

g. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

i. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his/her computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution

and possession of child pornography. Data that exists on a computer is particularly resilient to deletion.

j. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed and more on a particular user’s operating system, storage capacity, and computer habits.

**BACKGROUND ON CELLULAR PHONE AND CHILD
PORNOGRAPHY AND ONLINE CHILD EXPLOITATION**

7. Based upon my knowledge, training and experience in online child exploitation and child pornography investigations, as well as the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following:

- a. Cellular telephones have revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of online child exploitation.
- b. A cellular telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- c. The capability of a cellular telephone to store images in digital form makes the cellular telephone itself an ideal repository for child pornography. As explained further below, the storage capacity of electronic media used in home cellular telephones has

increased tremendously within the last several years. These drives can store extreme amounts of visual images at very high resolution.

d. The Internet, the World Wide Web and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.

e. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of cellular telephone files in any variety of formats. A user can set up an online storage account from any cellular telephone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's cellular telephone. And even in cases where online storage is used, evidence of child pornography can be found on the user's cellular telephone in most cases.

f. The interaction between software applications and the cellular telephone operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a cellular telephone hard drive without the user's knowledge. Even if the cellular telephone user is sophisticated and understands this automatic storage of information on his/her cellular telephone's storage, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the cellular telephone media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's cellular

telephone media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution and possession of child pornography.

**BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS IN
CHILD PORNOGRAPHY AND CHILD EXPLOITATION INVESTIGATIONS**

8. Based upon your affiant's training and experience and information related by agents and others involved in the forensic examination of computers, it is known that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. Your affiant also knows that during the search of the premises it is not always possible to adequately search the computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures

are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

9. Based on your affiant’s experience and consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer

system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

- a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and
- b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.
- c. Additionally, based upon your affiant's training and experience and information related by agents and others involved in the forensic examination of computers, your affiant knows that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be

"secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, it is known that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

10. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that segregating information before commencement of the review of digital evidence by the examining agent is inconsistent with the evidence assessment process in child pornography and online child exploitation investigations. This is true in part because the items to be searched will not only contain child pornography but also will contain the identity of the user/possessor of the child pornography as well as evidence as to the programs and software used to obtain the child pornography, which may be located throughout the areas to be searched.

a. As further described in Attachment B, this warrant seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how computers were used, the purpose of

their use, and who used them. Additionally, the warrant seeks information about the possible location of other evidence.

b. As described above and in Attachment B, this application seeks permission to search and seize certain records that might be found in or on the SUBJECT ITEMS, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

c. Although some of the records called for by this affidavit might be found in the form of user-generated documents (such as word processor, picture and movie files), computer hard drives can contain other forms of electronic evidence that are not user-generated. In particular, a computer hard drive may contain records of how a computer has been used, the purposes for which it was used and who has used these records, as described further in the attachments. For instance, based upon my knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know the following:

- i. Data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- ii. Virtual memory paging systems can leave traces of information on the hard drive that show what tasks and processes the computer were recently in use.

- iii. Web browsers, e-mail programs and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords.
 - iv. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices and the times the computer was in use.
 - v. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information may be evidence of a crime or indicate the existence and location of evidence in other locations on the hard drive.
- d. Further, in finding evidence of how a computer has been used, the purposes for which it was used and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a computer has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created, and, for example, by reviewing the Index.dat files (a system file that keeps track of historical activity conducted in the Internet Explorer application), whether a user accessed other information close in time to the file creation dates, times and sequences so as to establish user identity and exclude others from computer usage during times related to the criminal activity.
- e. Evidence of how a digital device has been used, what it has been used for and who has used it, may be the absence of particular data on a digital device and requires analysis

of the digital device as a whole to demonstrate the absence of particular data. Evidence of the absence of particular data on a digital device is not segregable from the digital device.

f. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge and intent.

g. This type of evidence is not “data” that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information is necessary to understand the evidence described in Attachment A also falls within the scope of the warrant.

SEARCH METHODOLOGY TO BE EMPLOYED

11. As noted within this search warrant, it would be extremely difficult, if not impossible to conduct a thorough on-site review of all of the potential evidence in this case. Given these constraints, the search methodology to be employed is as follows:

a. All computers, computer hardware and any form of electronic storage that could contain evidence described in this warrant will be seized for an off-site search for evidence that is described in the attachments of this warrant. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.

b. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

c. Additional techniques to be employed in analyzing the seized items will include (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas, (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and its attachments, and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.

12. Because it is expected that the computers, computer hardware and any form of electronic storage media may constitute (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case.

a. Because of the large storage capacity as well as the possibility of hidden data within the computers, computer hardware and any form of electronic storage media, it is anticipated that there will be no way to ensure that contraband-free evidence could be returned to the user/possessor of the computer, computer hardware or any form of electronic storage media, without first wiping such evidence clean. Wiping the original

evidence clean would mean that the original evidence would be destroyed and thus, would be detrimental to the investigation and prosecution of this case.

b. Further, because investigators cannot anticipate all potential defenses to the offenses in this affidavit, and as such, cannot anticipate the significance of the evidence that has been lawfully seized pursuant to this warrant, it is requested that all seized evidence be retained by law enforcement until the conclusion of legal proceedings or until other order of the court.

c. If after careful inspection investigators determine that such computers, computer hardware and electronic storage media do not contain (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO CONSPIRE TO
PRODUCE, DISTRIBUTE, POSSESS, AND/OR RECEIVE CHILD PORNOGRAPHY**

13. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who conspire to produce, distribute, possess, and/or receive child pornography. Such individuals:

a. May receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or

drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools.
- e. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of

names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

DETAILS OF THE INVESTIGATION

14. In February 2018, I was provided information from a a DHS/ICE/HSI undercover agent (hereinafter UCN Y agent) in Buffalo, New York regarding a Hamersville, Ohio suspect who posted child pornography through the internet. The postings occurred on Kik Messenger (KIK). KIK is an instant messaging application for mobile devices. The application is available on most iOS, Android, and Windows phone operating systems free of charge. KIK allows users to transmit and receive messages and share photos, sketches, mobile webpages, and other content. Specifically, between January 17 and January 19, 2018 the UCN Y agent observed KIK user “wayzombie” posting multiple images and videos of sexually explicit material depicting children into the KIK chat group, “Senior Yoga and Meditation”.

a. On or about January 18, 2018, KIK user “wayzombie” (display name: zombie way) posted a 14 second video file depicting a partially nude prepubescent female laying on a bed. The prepubescent female’s breast are covered by a blanket. During the video an adult penis can be seen attempting to penetrate the prepubescent female’s vagina. The prepubescent female’s face can also be seen during the video.

b. On or about January 19, 2018, KIK user “wayzombie” (display name: zombie way) posted an image file depicting a nude female toddler laying next to an adult female that

also appears to be nude. The adult female's fingers are spreading open the female toddlers vagina.

15. On January 22, 2018, a DHS administrative summons was served on KIK relating to user "wayzombie". KIK provided the following information about user "wayzombie":

First name: zombie

Last name: way

Email: wcusimano777@gmail.com (confirmed)

IP associated: 174.101.246.102

Device Model: LG-K371¹

Further investigation revealed that IP address 174.101.246.102 is operated by Charter Communications.

16. On January 30, 2018, a DHS Summons was served upon Charter Communications for subscriber records for the IP address 174.101.246.102 on dates and times corresponding to specific log-ins to the KIK user account "wayzombie". Charter Communications provided records indicating that IP address 174.101.246.102 was subscribed to by Wayne CUSIMANO at 9999 Fite Avenue in Hamersville, Ohio 45130.

17. On September 13th, 2018, an undercover detective from the Boone Police Department in North Carolina (hereinafter UC detective), began a proactive investigation into the sexual exploitation of children via KIK. The UC detective located a public KIK group displaying the name "No limits love" with the identifier of "#tab.oooo". The UC detective utilized an undercover KIK account and joined the aforementioned group. The UC detective was then vetted by an individual identified as KIK user "plain777". This vetting process included answering the

¹ This is the make and model of a LG brand smartphone.

question, "This is a yung to very yung share and chat group. Will u be offended if u see nude to very young" as well as sending a live picture to KIK user "plain777". The UC detective viewed that "plain777" had a gold badge on his profile picture, which indicated that he was a Group Administrator.

18. The following image and/or video files were observed by the UC detective, as posted by the KIK user "plain777" (display name: Plain Wayne), in the public KIK group #tab.oooo and later captured as evidence:

- a. On or about September 14th, 2018, KIK user "plain777" (display name: Plain Wayne) posted a 1 minute and 29 second color video file depicting a prepubescent female sitting on a toilet and masturbating with an unknown object. The female is wearing a shirt but is nude from the waist down and the camera is focused on the area of her genitals.
- b. On or about September 14th, 2018, KIK user "plain777" (display name: Plain Wayne) posted a 54 second color video file depicting a female child, approximately 5-years-old, performing oral sex on an adult male's erect penis.

Additionally, on or about September 14th, 2018 KIK user "plain777" (display name: Plain Wayne) posted 3 images and two additional videos depicting what appears to be child pornography.

- c. On or about September 15th, 2018, KIK user "plain777" (display name: Plain Wayne) posted an image file depicting a nude prepubescent female, approximately 7-years-old, lying on her back on the floor. The female's legs are spread, displaying her genitals in a lewd and lascivious manner. What appears to be ejaculate is seen in and around the area of the female child's genitals.

- d. On or about September 15th, 2018, KIK user "plain777" (display name: Plain Wayne) posted two additional image files depicting what appears to be child pornography.
 - e. On or about September 17th, 2018, KIK user "plain777" (display name: Plain Wayne) posted a 1 minute and 2 second color video file depicting a clothed adult female with a nude prepubescent female sitting on her lap. Both the adult female and minor female are facing the camera. The nude female child, approximately 8-years-old, has her arms under her knees and is spreading her legs, which displays her genitals in a lewd and lascivious manner. Throughout the entirety of the video, the adult female uses her right hand to rub the genitals of the female child.
 - f. On or about September 17th, 2018, KIK user "plain777" (display name: Plain Wayne) posted an additional image file and two video files depicting what appears to be child pornography.
 - g. On or about September 20th, 2018, KIK user "plain777" (display name: Plain Wayne) posted an image file depicting an adult male lying on his back, while a nude prepubescent female, approximately 10-years-old, performs oral sex on him. The nude female child is crouched on her hands and knees above the adult male, with her head facing towards his genitals, while his face is near her genitals.
19. On September 17, 2018, a North Carolina State Bureau of Investigation Administrative Subpoena was served on KIK relating to user "plain777". KIK provided the following information about user "plain777":
- First name: Plain
- Last name: Wayne
- Email: waynepain65@gmail.com (unconfirmed)

IP associated: 71.65.69.218

Device Model: LG-K371

Further investigation revealed that IP address 71.65.69.218 is operated by Charter Communications.

20. On September 19, 2018, a North Carolina State Bureau of Investigation Administrative Subpoena was served upon Charter Communications for subscriber records for the IP address 71.65.69.218 on dates and times corresponding to specific log-ins to the KIK user account "plain777". Charter Communications provided records indicating that IP address 71.65.69.218 was subscribed to by Jane Landry at 9999 Fite Avenue in Hamersville, Ohio 45130.

21. On September 27, 2018, your affiant reviewed Ohio driver license records. On September 19, 2018, Wayne CUSIMANO was issued an Ohio driver license registered to 9999 Fite Avenue in Hamersville, Ohio.

22. On September 27, 2018, your affiant observed Wayne CUSIMANO step out of the front door of house at 9999 Fite Avenue in Hamersville, Ohio.

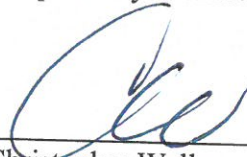
CONCLUSION

23. Based on the above information, there is probable cause to believe that of Title 18, United States Code, Sections 2252(a)(2)(B) and 2252A(a)(2) (distribution and receipt of child pornography), and Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(5)(B) (possession of child pornography) have been violated, and that the property, evidence, fruits and instrumentalities of these offenses listed in Attachment B, which is incorporated herein by reference, is located at the SUBJECT PREMISES.

24. Based upon the foregoing, your Affiant respectfully requests that this Court issue a search warrant for the SUBJECT PREMISES more particularly described in Attachment A,

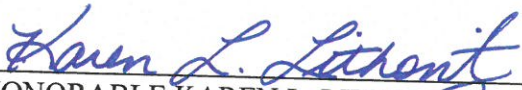
authorizing the seizure of the items described in Attachment B which is incorporated herein by reference.

Respectfully submitted,



Christopher Wallace
Special Agent
ICE Homeland Security Investigations

Subscribed and sworn before me this 1st day of October, 2018.



HONORABLE KAREN L. LITKOVITZ
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

**DESCRIPTION OF THE PERSON, PROPERTY,
AND ITEMS TO BE SEARCHED**

PERSON AND PROPERTY:

The property is located at 9999 Fite Avenue, Hamersville, Ohio 45342 and is a single family house with white siding. The house is located at the corner of Fite Avenue and Wooster Avenue in Hamersville, Ohio. See below photograph of the front of the house.



The property includes a Blue Ford SUV with Ohio Temporary Tag G875296 parked on the property (also pictured above).

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

Items evidencing violations of Title 18, United States Code, Sections 2252 and 2252A (possession, receipt, and distribution of child pornography), including but not limited to the following:

Computers and Electronic Media

1. Any cellphones, computers, or computer hardware/media/software. Including a LG smartphone, model number: LG-K371. The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space. The seizure and search of cellphones, computers, and computer media will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is

capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents, and materials referencing or relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records

9. Any records related to the possession, receipt, and distribution of child pornography.

10. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed and/or traded.

11. Any Internet or cellular telephone communications (including email, social media, etc.) with minors.

12. Evidence of the use of KIK and any communications from KIK.

13. Evidence of the utilization of peer-to-peer file sharing programs.
14. Evidence of utilization of email accounts, social media accounts, and online chat programs.
15. Evidence of utilization of other user names or aliases.
16. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, diaries, and reference materials.
17. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.
18. Records of address or identifying information for individuals using computers located at 9999 Fite Avenue, Hamersville, Ohio 45130, and any personal or business contacts or associates of theirs, (however and wherever written, stored, or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user IDs, eIDs (electronic ID numbers), and passwords.

Materials Relating to Child Pornography, Child Erotica, and Depictions of Minors

19. Any child pornography.
20. Any and all visual depictions of minors.
21. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
22. Any books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the

transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

23. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

24. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

Other Records

25. Lists of computer and Internet accounts, including user names and passwords.

26. Any information related to the use of aliases.

27. Documents and records regarding the ownership and/or possession of the searched premises.

28. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

Photographs of Search

29. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.